Improving an algorithm for factorizing polynomials over a finite field and constructing large irreductible polynomials

Paul Camion

INRIA

CENTRE DE ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P.105
78153 Le Chesnay Cedex
France
Tél.: 954 90 20

Rapports de Recherche

N° 152

IMPROVING AN ALGORITHM FOR FACTORIZING POLYNOMIALS OVER A FINITE FIELD AND CONSTRUCTING LARGE IRREDUCTIBLE POLYNOMIALS

Paul CAMION

Juillet 1982

IMPROVING AN ALGORITHM FOR FACTORIZING POLYNOMIALS OVER A FINITE FIELD

AND CONSTRUCTING LARGE IRREDUCIBLE POLYNOMIALS

by Paul CAMION

Abstract

Let $f(X) \in \mathbb{F}_q[X]$ be a polynomial with simple roots to be factorized. The so-called Berlekamp subalgebra B spanned over $\mathbb{F}_q$ by the idempotents of $A = \mathbb{F}_q[X]/(f(X))$ is considered. An exponential technique previously introduced based upon taking at random elements from B led to obtained idempotents and, from that, to getting all the factors of f(X). This algorithm is speeded up in three ways. The concept of separating subset of B is introduced and the operator of Mc ELIECE mapping A onto B is used for contructing a small separating set. Factorizing subsets of $\mathbb{F}_q$ were previously defined and investigated. The algorithm and those objets are used together with a process introduced by F.J. Mc WILLIAMS for a fast construction of primitive idempotents.

Afterwards, an algorithm is introduced for constructing irreducible polynomials of $\mathbb{F}_q[X]$ of degree d, for large values of d, in which the most expensive operation is the Euclidian algorithm applied to two polynomials of degree 2d.

Résumé

Soit $f(X) \in \mathbb{F}_q[X]$ un polynôme à racines simples devant être factorisé. On considère la sous-algèbre B, dite de Berlekamp, qui est engendrée sur $\mathbb{F}_q$ par les idempotents de $A = \mathbb{F}_q[X]/(f(X))$. Une technique exponentielle introduite précédemment basée sur un tirage aléatoire d'éléments de B menait à l'obtention d'idempotents et, de là, à la construction de tous les facteurs de f(X). Cet algorithme est accéléré de trois manières. La notion de partie séparatrice de B est introduite et l'opérateur de Mc ELIECE qui envoie A sur B est utilisé pour construire une partie séparatrice petite. Les parties factorisantes de $\mathbb{F}_q$ furent précédemment définies et étudiés. L'algorithme mentionné et ces deux objets et un processus introduit par F.J. Mc WILLIAMS sont utilisés conjointement dans le but d'obtenir une construction rapide de tous les idempotents primitifs.

On introduit pour suivre un algorithme de construction de polynômes de $\mathbb{F}_q[X]$ irréductibles de degré d, pour de grandes valeurs de d, dans lequel l'opération la plus coûteuse est l'algorithme d'Euclide appliqué à deux polynômes de degré 2d.

0. - INTRODUCTION

In P. CAMION [4] and [5], we introduced an algorithm for constructing the primitive idempotents of any ideal of $A = \mathbb{F}_q[X_1,\ldots,X_r]/(t_1(X_1),\ldots,t_r(X_r))$ in the case where all $t_i(X_i)$, $i = 1,\ldots,r$, have simple roots. For $r = 1$, that algorithm allows the factorization of any $f(X) \in \mathbb{F}_q[X]$ for whatever finite filed $\mathbb{F}_q$. The basic idea is the following. Let $e_1,\ldots,e_k$ be the primitive idempotents of A. Then we consider the $\mathbb{F}_q$-subalgebra B of A, $B = \bigoplus_{1\le i\le k} \mathbb{F}_q\, e_i$ which is called the Berlekamp Algebra of A. The algorithm of BERLEKAMP [3] allows the construction of a basis N of B as well as the operator T of Mc ELIECE [10] which works very efficiently when the irreducible factors of $t_1(X_1),\ldots,t_r(X_r)$ all have degree t [8]. If u is an idempotent of A, then u N contains a basis N' of $(u) \cap B = \bigoplus_{i\in I} \mathbb{F}_q\, e_i$, where $u = \sum_{i\in I} e_i$

i) 1^{th} case, q is odd. For every w in $(u) \cap B$, then w^{2d}, where $d = (q-1)/2$ is an idempotent. Let $w = \sum_{i\in I} a_i\, e_i$. Then w^d has components 0, -1 and 1 in $\{e_i\}_{i\in I}$; components -1 appear whenever some a_i's are non-squares in $\mathbb{F}_q$. If w^d has both components 1 and -1, then $u = w^d(w^d+u)/2 + (u-w^d(w^d+u)/2)$ is the sum of two orthogonal idempotents.

ii) 2^d case, q is even. If q is 2^{2i+1}, then we consider $q' = q^2$, else $q' = q$. Here, w will be taken with $a_i \in \mathbb{F}'_q$, $i \in I$, which is done by taking a linear combination in N' over $\mathbb{F}'_q$. Here $d = (q'-1)/3$ and we also obtain recurrently, picking up w's at random, the decomposition $u = \sum_{i\in I} e_i$.

This is outlined very roughly. The reader is invited to see [4], [5] and [6].

Here we confine ourself to factorizing polynomials and constructing irreducible polynomials of high degrees.

In both cases, we obtain deterministic algorithms for a given field $\mathbb{F}_q$.

Notice that the idea of using idempotents for factorizing a polynomial goes back to F.J. Mac WILLIAMS [11]. In the case where $A = \mathbb{F}_2[X]/(X^n+1)$, n odd, a basis of B is easily constructed. Indeed, if X^n+1 has k irreducible factors, then the dimension of B over $\mathbb{F}_2$ is k since every minimal ideal $(g_i(X))$ of A, where $g_i(X) = (X^n+1)/f_i(X)$ and $f_i(X)$ is an irreducible factor of X^n+1, i=1,...,k, contains a unique primitive idempotent e_i. Then constructing k linearly independent idempotents provides a basis of B. But the set of non-zero elements in $\mathbb{Z}/(n)$ is partitioned into k cyclotomic classes, $C_0=\{1\}$, $C_1=\{2,4,\ldots\}$, $C_2=\{3,6,\ldots\}$,... Now to each C_i corresponds an idempotent $u_i=\sum_{j\in C_i} X^j$, and $u_0,\ldots,u_{k-1}$ are linearly independent since any two of them have disjoint sets of non-zero terms. Finally an algorithm is given [11] for obtaining ℓ_i, i=1,...,k from the set $\{u_0,\ldots,u_{k-1}\}$. We will see in the following pages that the algorithm suggested by D. LAZARD is essentially the same as this one which is adapted to the case where $A = \mathbb{F}_q[X]/(f(X))$ where f(X) has distinct roots. Account of [11] is found in v. LINT's "Coding Theory", Springer-Verlag §201. Obtaining the primitive idempotents solves the problem of factorizing f(X) since the set of irreducible factors of f(X) is $\{(e_i-1,f(X))\}_{1\le i\le k}$.

1. - FACTORIZING POLYNOMIALS

1.1. - The Mc Eliece operator

The polynomial $f(X) \in \mathbb{F}_q[X]$ may be assumed to have distinct roots (for example Mc ELIECE [10]). We then compute $(X^{q^i} - X, f(X))$, $i = 1,2, \ldots$ up to the value t for which we obtain a g.c.d., $g(X) \neq 1$, of which all irreducible factors then have degree t. We keep the values X^{q^i} mod $f(X)$, $i = 1,\ldots,t-1$ and reducethose polynomials modulo $g(X)$. Henceforth $f(X)$ has distinct roots and all its irreducible factors have degree t. Consequently the operator T of Mc ELIECE is easily defined as follows. For every $v(X) \in A = \mathbb{F}_q[X]/(f(x))$, then $Tv = \sum_{o \leq i < t} v(X^{q^i})$. We first have :

Theorem 0 : The operator T maps A onto B [10] and [8]

Let n be the degree of $f(X)$.

Co ollary . The set $T\{1,X,X^2,\ldots,X^{n-1}\}$ contains a basis of B.

Notice that, keeping the values $X^j, X^{jq}, \ldots, X^{jq^{t-1}}$ mod $f(X)$ when computing TX^j allows the computation of TX^{j+q^i}, $i = 0,1,\ldots$ by means of t products mod $f(X)$, since $X, X^q, \ldots, X^{q^{t-1}}$ have already been computed when reducing the problem as told hereabove.

1.2. - Proving the existence of a deterministic algorithm in $O((\log_2 q)\ \dim B)$

Definition 1 : A subset S of B is separating when for every idempotent u of A with the form $e_i + e_j$, $i<j$, there exist at least a v in S such that $uv = a_i e_i + a_j e_j$, with $a_i \neq a_j$.

Clearly, any set containing a basis of B is a separating set, but more particularly, we have the following theorem 1.

Theorem 1 : The set $\{TX, TX^2, \ldots, TX^{2t-1}\}$ is separating, and if $q = 2$, the set $\{TX, TX^3, \ldots, TX^j\}$ for $j = 2\ t-1$ is separating.

The proof is in appendix 1.

We also say that v separates the idempotent u if uv is not a scalar multiple of u.

Definition 2. Let q be odd. Then a subset P of $\mathbb{F}_q^*$ is factorizing if for every two subset {a,b} of $\mathbb{F}_q$, there exist an x in P $\cup \{0\}$ such that $(a+x)(b+x)$ is zero or a non-square.

Let q be an even power of 2. Now $\mathbb{F}_q^*$ contains a subgroup C_o of index 3. Then a subset P of $\mathbb{F}_q^*$ is factorizing if for every two-subset {a,b} of $\mathbb{F}_q$, there exist an x in P $\cup \{0\}$ such that $(a+x)(b+x)$ is zero or $a+x$ and $b+x$ are not in a same coset of C_o.

Theorem 2 [6] : For q odd, there exist a factorizing subset P of $\mathbb{F}_q^*$ such that :

(1) $\quad \text{Card } P < 2 \log_2 q.$

For q an even power of 2, there exist a factorizing subset P of $\mathbb{F}_q^*$ such that :

(2) $\quad \text{Card } P < \log_3 (3\ q^2/2).$

In the first case, every factorizing subset P verifies :

(3) $\quad \log_2 q < \text{Card } P + 2,$

and in the second case, every factorizing subset P verifies :

(4) $\quad \log_3 q < \text{Card } P + 2.$

Now, if we are faced with the problem of factorizing polynomials over a given, fixed finite field, for example for finding the roots of an error-locating polynomial, we will first determine a factorizing subset P of $\mathbb{F}_q$. Then we don't need any longer constructing a basis of B. When having to decompose a non-primitive idempotent u into a sum of orthogonal idempotents we only need to find a $v \in B$ separating u. Thatfor, we try TX, TX^2,...

Notice that the average number of tries is at most $q/(q-1)$. Also if q is 2^{2i+1} all the above computations are performed in $\mathbb{F}_q[X]$, but P is determined in $\mathbb{F}_{q'}$, $q' = q^2$. Now we are certain that for at least one x in $P \cup \{0\}$, then $w = vu + x$ will yield a decomposition of u as recalled in i) and ii).

1.3. - Back to probabilistic algorithms

1.3.1. - Checking the end

Each time we get an idempotent u, we have to see if it is primitive. In [4] and [5] we suggested to first construct a basis N of the BERLEKAMP algebra B of A. There, u is primitive iff the set uN has rank 1. In [8] we worked with an f(X) all of which irreducible factors had degree t. There, u is primitive iff $(1-u, f(X))$ has degree t. In all those papers, the idea was to decompose 1 into the sum of the k primitive idempotents in k-1 steps. At each step, a non-primitive idempotent is decomposed into a sum of two orthogonal idempotents.

D. Lazard [15] suggest the following faster probabilistic algorithm. Suppose we are given any way of producing idempotents of A at random. Notice that if all irreducible factors of f(X) have degree t, then the number of primitive idempotents of A is $n/t = k$, which is known.

1.3.2. - Lazard's algorithm

Step 1 : $E_1 = \{1\}$

Step i : If Card $E_{i-1} = k$, then end, else an idempotent u is produced. For every x in E_{i-1}, compute ux and $(1-u)x$. The set of non-zero polynomials obtained will form E_i.

End

Notice that E_i is a set of orthogonal idempotents, thus an idempotent is never obtained twice in the process of forming E_{i+1}. That algorithm was investigated by P. FLAJOLET and J.M. STEYAERT [16]. Let us assume that for every idempotent $u = \sum_{1 \le i \le k} a_i e_i$ produced and for every i, then the probability that a_i be 1 is π. Their result is as follows :

$$(5) \qquad \lim_{k \to \infty} \frac{\bar{H}_k}{\log_2 k} = \frac{2}{\log_2(\pi^2 + (1-\pi)^2)^{-1}}$$

where $\bar{H}_k$ is the average number of steps in Lazard's algorithm to obtain all k primitive idempotents. Notice that for $\pi = 1/2$, then $\bar{H}_k \sim 2 \log_2 k$.

1.3.3. - Taking the idempotents u from a smaller set

Observe that Lazard's algorithm ends as soon as the set of idempotents u produced form a separating set. The two distinct components in definition 1 are 0 and 1.

Let us show by an example that it may be worthwile to take the idempotents u from a smaller set than the set of all idempotents.

Let t be a prime, $q = 2$, $n = 2^t - 2$ and $f(X) = \sum_{0 \le i \le n} X^i$. We know that f(X) factors into $n/t = k$ irreducible polynomials of degree t. Here theorem 1 gives us a separating set of t idempotents of A. Using that set for Lazard's algorithm, it will end in at most t steps. If we had to take the idempotents u at random, assuming that π is close to 1/2, the average number of steps would be approximately $2 \log_2 k > 2t - 2 - 2 \log_2 t$.

That example shows that theorem 1 is close to best possible for $q = 2$ since the smallest size for a separating set is $\lceil \log_2 k \rceil$.

Observe that a separating set $S \subset B$ of size s for an algebra A with k primitive idempotents may be considered a kxs matrix with entries in $\mathbb{F}_q$ in which any two rows are distinct. If we assume that each entry of a kxs matrix is uniformly distributed over $\mathbb{F}_q$, the probability for such a matrix to yield a separating set is :

(6) $$q^s(q^s-1)\ \ldots\ (q^s-k+1)/q^{ks}.$$

Now if a separating set S is taken at random among all possible separating sets of size s, then the probability that i given elements in that set form in its turn a separating set is :

(7) $$q^{k(s-i)}\ q^i(q^i-1)\ \ldots\ (q^i-k+1)/q^s(q^s-1)\ \ldots\ (q^s-k+1).$$

For example if f(X) is a product of k = 4 irreducible factors of degree t= 7, then it is reasonable to expect that the probability for the set $\{TX, TX^3, TX^5, TX^7\}$ to end Lazard's algorithm is :

(8) $$2^{4\times 3}.2^4(2^4-1)(2^4-2)(2^4-3)/2^7(2^7-1)(2^7-2)(2^7-3) = .698$$

in place of :

(9) $$2^4(2^4-1)(2^4-2)(2^4-3)/2^{4\times 4} = .666$$

for a random set of four idempotents u.

1.4. - Conclusion

LAZARD's improvement of the algorithm introduced in [4] and [5] should apparently be adopted for finding the primitive idempotents of an ideal of a semi-simple algebra $A = \mathbb{F}_q[X_1,\ldots,X_r]/(t_1(X_1),\ldots,t_r(X_r))$ in all cases, i.e., $r\geq 1$, q a power of 2, q a small add prime, or q a large odd prime.

What is left to decide is how to produce the random idempotents required. The first method introduced and outlined in i) and ii) is expensive because it requires the diagonalization of a matrix by Berlekamp's algorithm which need $O(n^3)$ operations in $\mathbb{F}_q$ for the problem of factorizing a polynomial $f(X) \in \mathbb{F}_q[X]$ of degree n.The other method suggested in [15] consist in taking w from A and constructing the idempotent $w^d(w^d+1)/2$, $d = (q^t-1)/2$, where t is the degree of every irreductible factor of f(X). This require approximately $1.5\ t\ \log_2 q$ products of polynomials mod f(X).

Now if we considered the set $S = \{TX, TX^2, \ldots, TX^{2t-1}\}$ then we have seen that taking successively w from $S + \mathbb{F}_q$ or from $S + (P \cup \{0\})$ whenever q is fixed and not to large, with P a factorizing subset of $\mathbb{F}_q$ or $\mathbb{F}_{q'}$ is somewhat better that taking w at random from B. Constructing an element from S need t products mod f(X) and then computing w^d, where $d = (q-1)/2$, $(q-1)/3$ or $(q^2-1)/3$ according to whether q is odd, q is an even power of 2 or q is an odd power of 2, respectively, need approximately $1.5 \log_2 q$ products of polynomials mod f(X). We clearly have to comparate $t + 1.5 \log_2 q$ with $1.5\, t \log_2 q$.

Finally, when the primitive idempotents $e_1, \ldots, e_k$ of $A = \mathbb{F}_q[X]/(f(X))$ are obtained then g.c.d. $(1-e_i, f(X))$ is computed, $i = 1, \ldots, k$. Those are the irreducible factors of f(X).

2. - CONSTRUCTING IRREDUCTIBLE POLYNOMIALS OF HIGH DEGREES

2.1. - An easy construction for some very particular irreducible polynomials

The simplest way of constructing an irreducible polynomial over $\mathbb{F}_q$ is apparently to just take the irreducible polynomial $(X^r-1)/(X-1)$ for r a prime for which q is primitive mod r.

The corollary of theorem 3 in appendix 1 allows an easy factorization of the cyclotomic polynomial $F_m(X)$ over $\mathbb{F}_2$ when m is a certain product of two primes.

Appendix II allows an easy construction of $F_m(X)$ when knowing $F_{m_1}(X)$ and $F_{m_2}(X)$, $m_1 m_2 = m$, $(m_1, m_2) = 1$. For, $F_{m_1}(Z)$ being f(Z), systems (2) and (3) are easily solved for $(x_1, \ldots, x_d) = (\sigma_1, \ldots, \sigma_d)$ and the integers $a_1, \ldots, a_{\phi(m)}$ are obtained. The same is done for $F_{m_2}(Z) = f(Z)$ giving the corresponding integers $a'_1, \ldots, a'_{\phi(m)}$. Now the products $a_1 a'_1, \ldots, a_{\phi(m)} a'_{\phi(m)}$ are computed which are substituted for $a_1, \ldots, a_d$, $d = \phi(m)$ in (2). This gives $x_1, \ldots x_d$ in $O(d^2)$ operations. Notice that the absolute values of $a'_1, \ldots, a'_{\phi(m)}$ are bounded by $\phi(m)$.

We shall observe that the factors of Z^m-1, for all integers m are the only polynomials verifying the hypothesis on f(Z) for which the sequence $(|a_i|)_{i\in\mathbb{N}}$ is bounded. For, if $(|a_i|)_{i\in\mathbb{N}}$ is bounded, it should be ultimately periodic, with period, say, m, since $(a_i)_{i\in\mathbb{N}}$ verifies a linear recurrence. Hence $(Z^m-1)f'(Z)/f(Z)$ is a polynomial and since $(f'(Z), f(Z)) = 1$, then f(Z) divides Z^m-1.

2.2. - Other constructions

2.2.1. - The basic property used

If f(Z) is given in (1), of appendix 2, we know that a_i is the sum of the i^{th} powers of the inverses of its roots whenever f(Z) has distinct roots. See for example F.J. Mac WILLIAMS and N.J.A. SLOANES [17]. Let us denote by $\tilde{f}(Z)$ the reciprocal polynomial of f(Z).

Consequently, if :

$$(1) \qquad P_1(Z) = -\sum_{i\in\mathbb{N}} a_i Z^i \quad \text{and} \quad P_2(Z) = -\sum_{i\in\mathbb{N}} b_i Z^i$$

are the R.H.S. of (1) for $f(Z) = f_1(Z)$ and $f(Z) = f_2(Z)$ respectively, $f_j(Z)$ having distinct roots, $j = 1,2$, then the product a_ib_i is the sum of the i^{th} powers of all possible products of a root of $\tilde{f}_1(Z)$ with a root of $\tilde{f}_2(Z)$. Let $\{\alpha_1,\ldots,\alpha_r\}$ be the set of roots of $f_1(Z)$ and $\{\beta_1,\ldots,\beta_s\}$ that one of $f_2(Z)$ and $g(Z) = \prod_{\substack{1\le i\le r\\ 1\le j\le s}} (Z - \alpha_i\beta_j)$. If moreover g(Z) has also distinct roots, we then have that :

$$(2) \qquad Z\, g'(Z)/g(Z) = -\sum_{i\in\mathbb{N}} a_i b_i Z^i.$$

Example : Let $f_1(Z)$ and $f_2(Z)$ be irreducible polynomials in $\mathbb{F}_q[Z]$ and $(r,s) = 1$. Then clearly $(\alpha_1\beta_1)^{q^j}$ runs over all roots of g(Z) which is consequently irreducible and has degree rs.

2.2.2. - First construction

Considering the polynomials $f_1(Z)$ and $f_2(Z)$ from the example, we first compute the sequences $(a_1, a_2,\ldots,a_{rs})$ and $(b_1,b_2,\ldots,b_{rs})$ from (2), (3) of appendix 2 and the subsequent relations. Afterwards the sequence

$(a_1 b_1, a_2 b_2, \ldots, a_{rs} b_{rs})$ is computed. Now system (3) for d = rs allows the computing of $x_0, x_1, \ldots, x_{rs}$, which are the coefficients of g(Z), in $O((rs)^3)$ operations in $\mathbb{F}_q$.

Notice that if $f_1(Z)$ and $f_2(Z)$ are primitive, then g(Z) belongs to the exponent :

$$(3) \qquad (q^r - 1)(q^s - 1)/(q-1)^2.$$

2.2.3. - Operating over the integers

Consider now the polynomials $f_1(X)$ and $f_2(X)$ as belonging to $\mathbb{Z}[X]$ for q a prime. Then they are necessarily irreducible in $\mathbb{Z}[X]$ and $g(X) \in \mathbb{F}_q[X]$ may be obtained by taking mod q the polynomial $g^*(X) \in \mathbb{Z}[X]$ of which the roots are all possible products of a root of $f_1(X)$ and a root of $f_2(X)$. To see this easily, it is enough to observe that $g^*(X)$ is the characteristic polynomial of the Kronecker product of the companion matrices of $f_1(X)$ and $f_2(X)$. Computing mod q may be done from the beginning or when obtaining $g^*(X)$. In both cases g(X) is obtained.

It is impossible that $g^*(X)$ had repeated roots since it would then be reducible and g(X) would be reducible. Consequently $g^*(X)$ may be computed as for the construction of the cyclotomic polynomials by handling system (2). This is done in $O((rs)^2)$ operations in $\mathbb{Z}$.

That method seems attractive since $g^*(X)$ is computed in $O((rs)^2)$ operations in $\mathbb{Z}$ for a given couple of irreducible polynomials $f_1(X)$ and $f_2(X)$ over a prime field $\mathbb{F}_q$ with relatively prime degrees r and s. However if α is the complex root with the largest module of $f_1(X)$, then $|\alpha| \geq 1$, and we have just seen that $|\alpha| = 1$ iff $f_1(X)$ is a cyclotomic polynomial since for $Xf_1'(X)/f_1(X) = \sum_{i \geq 1} a_i X^i$, then the integer a_i is the sum of the i^{th} powers of the roots of $f_1(X)$. In other words, a_i grows as does $|\alpha|^i$.

However, let us consider a polynomial $f_1(X)$ or $f_2(X)$ with the form :

$$(4) \qquad f(X) = X^d - X^j - a_{j-1} X^{j-1} - a_{j-2} X^{j-2} - \ldots - 1,$$

where the a_i's are all 0 or 1. The companion matrix of such a polynomial is non-negative. Then the theory of FROBENIUS asserts that the root with the largest module is real and positive. Let α be that positive root and let β be the positive root of the polynomial :

$$(5) \qquad X^d - a\,X^j - 1,$$

where $a = -f(1)$. Then clearly $\alpha \leq \beta$. But since $\beta^j(\beta^{d-j} - a) = 1$, then $\beta^{d-j} - a < 1$; $\beta < (a+1)^{1/(d-j)}$.

Consequently, if $d-j$ is large and a small, then the growth of a_i will not be too fast.

2.2.4. - An algorithm which only need one application of the Euclidian algorithm to two polynomials of degree 2d and $O(\log(q-1)+\log\log d)$ products in $\mathbb{F}_q[X]$ for constructing an irreducible polynomial $g(X)\in\mathbb{F}_q[X]$ of degree $d=rs$, $(r,s)=1$, when knowing irreducible polynomials of degree r and s respectively.

The algorithm that we describe here should apparently be prefered to the previous two ones. It relies upon the one for finding the error locator polynomial and the error evaluator polynomial in decoding alternant codes ([17], Ch. 12, § 9)

Let $r_{-1}(X)$ and $r_0(X)$ be given in $\mathbb{F}_q[X]$ and $r_{-1}(X) = r_0(X)\ q_0(X) + r_1(X), \ldots, r_{i-1}(X) = r_i(X)\ q_i(X) + r_{i+1}(X)$, where the degree of $r_{i+1}(X)$ is less than the degree of $r_i(X)$. Then there exist a smallest integer s such that $r_{s+1}(X) = 0$ and we know that $r_s(X) = (r_{-1}(X), r_0(X))$.

We call $r_i(X)$ the i^{th} remainder of the sequence based upon the couple $(r_{-1}(X), r_0(X))$. For the application that we have in view we restate part of Theorem 16 of [17], Chap. 12, § 9 as follows

Theorem : Let K be a field and p(X), q(X) be given in K[X] with $(p(X),q(X))=1$. Moreover the degree of q(X) is d and that one of p(X) is less than d.

Suppose that

$$p(X) \equiv q(X)\ S(X) \bmod X^{2d} \tag{6}$$

where

$$S(X) = \sum_{0\le j<2d} s_j\ X^j \neq 0. \tag{7}$$

Let k be the smallest i for which the remainder $r_i(X)$ of the sequence based upon $(r_{-1}(X), r_0(X)) = (X^{2d}, S(X))$ has degree less than d. Then $r_k(X) = \delta p(X)$ for some $\delta\in K^*$.

Notice that the authors in [17] would also obtain $\delta q(X)$ by proceeding with the so-called "extended" Euclidian algorithm which need keeping the quotients $q_i(X)$ when computing $r_{i+1}(X)$ and performing $O(d)$ extra products of polynomials.

Since $S(X)$ is invertible mod X^{2d}, we will avoid this by computing

$$\delta q(X) \equiv \delta p(X)\, S^{-1}(X) \bmod X^{d+1}. \tag{8}$$

This will need an average of

$$1{,}5\, \log_2(q-1) + \left\lceil \log_2 \left\lceil \log_q(d+1) \right\rceil \right\rceil + 1 \tag{9}$$

products of polynomials and would speed up as well the decoding process of alternant codes. This relies on the following

Lemma : Let $f(X)$ be a polynomial of degree less than r in $\mathbb{F}_q[X]$. Then

$$f^{-1}(X) \equiv f^t(X) \bmod X^r,$$

where $t=q^s-1$, $s= \left\lceil \log_q r \right\rceil$.

Since s is the smallest integer such that $q^s \geq r$, we have that $f^{q^s}(X) = f(X^{q^s}) \equiv 1 \bmod X^r$. □

Then (9) follows from the fact that calculating $f^{q-1}(X)$ need an average of $1{,}5\, \log_2(q-1)$ products and $f^{(q-1)q^i}(X) = f^{(q-1)}(X^{q^i})$ is obtained by shifting.

Since $q^s-1 = q-1 + (q-1)q + \ldots + (q-1)q^{s-1}$, then computing $f^t(X) \bmod X^r$ need on the average $1{,}5\, \log_2(q-1) + \left\lceil \log_2 \left\lceil \log_q r \right\rceil \right\rceil$ products mod X^r.

Finally, the congruence (8) is mod X^{d+1} in place of X^{2d} since the obtained $\delta q(X)$ is known to have degree d.

The algorithm

We proceed as is 2.2.2. except that the sequences (a_i) and (b_i) are computed up to $a_{2rs} = a_{2d}$ and $b_{2rs} = b_{2d}$ respectively. The lemma may be used to speed up then calculation by computing $f_1'(X)\ f_1^{-1}(X) \bmod X^{2d}$ and $f_2'(X)\ f_2^{-1}(X) \bmod X^{2d}$.

Then the polynomial

$$S(X) = a_1b_1 + a_2b_2\ X + \ldots + a_{2d}b_{2d}\ X^{2d-1}$$

is obtained, and since

$$\frac{g'(X)}{g(X)} \equiv S(X) \bmod X^{2d},$$

then the theorem and the lemma allow the computation of $g'(X)$ and $g(X)$ respectively.

Example

Let $f_1(X) = 1 + X + X^2$ and $f_2(X) = 1 + X + X^3$, both in $\mathbb{F}_2[X]$.

$$\frac{f_1'(X)}{f_1(X)} \equiv 1 + X + X^3 + X^4 + X^6 + X^7 + X^9 + X^{10} \bmod X^{12}$$

$$\frac{f_2'(X)}{f_2(X)} \equiv 1 + X + X^3 + X^6 + X^7 + X^8 + X^{10} \bmod X^{12}.$$

Then

$$\frac{g'(X)}{g(X)} \equiv 1 + X + X^3 + X^6 + X^7 + X^{10} \bmod X^{12} \equiv S(X) \bmod X^{12}.$$

Proceeding with the Euclidean algorithm based upon the couple $(r_{-1}(X), r_0(X)) = (X^{12}, S(X))$, we find out $r_1(X) = X^2+X^3+X^5+X^8+X^9$, $r_2(X) = 1+X+X^2+X^3+X^4+X^5+X^7+X^8$, $r_3(X) = x+X^4+X^6$, $r_4(X) = 1$.

Hence $g'(X) = 1$ and $g(X) \equiv S^{-1}(X) \bmod X^{12}$, or $g(X) \equiv S^{-1}(X) \bmod X^7$, since d=6.

By the lemma, we obtain g(X) with only two products :

$$g(X) \equiv (1+X+X^3+X^6)\ (1+X^2+X^6)\ (1+X^4) \bmod X^7$$

$$g(X) = 1 + X + X^2 + X^4 + X^6.$$

Remark

For q=2, interpreting the algorithm for fast division of [19], page 288, would lead to the following process for calculating the inverse of $a(X) = a_0 + a_1X +\ldots+ a_{2^s-1}X^{2^s-1}$ modulo X^{2^s}.

$$a_0 + a_1X = a_1(X)$$

$$a_1^2(X)\ (a_0+a_1X+a_2X^2+a_3X^3) \equiv a_2(X) \bmod X^4$$

$$a_2^2(X)\ (a_0+a_1X +\ldots+ a_7X^7) \equiv a_3(X) \bmod X^8$$

$$a_{s-1}^2(X)\ (a_0+a_1X +\ldots+ a_{2^s-1}X^{2^s-1}) \equiv a^t(X) \equiv a^{-1}(X) \bmod X^{2^s}.$$

In the example, we would compute

$$a_1(X) = 1+X\ ;\ a_1^2(X)(1+X+X^3) \equiv a_2(X) \equiv 1+X+X^2 \bmod X^4,$$

and

$$a_2^2(X)\ (1+X+X^3+X^6) \equiv 1+X+X^2+X^4+X^6 \bmod X^8.$$

Reducing mod X^{d+1} may be done at the end.

2.2.5. - Passing from an irreducible polynomial to another

Let $g(X) = a_0 + a_1 X + \ldots + a_{d-1} X^{d-1} + X^d$ be an irreducible polynomial over $\mathbb{F}_q$ and let α be one of its roots in $\mathbb{F}_{q^d}$. There is a representation of $\mathbb{F}_{q^d}$ by matrices in which α is the matrix

$$\begin{vmatrix} 0 & 0 & \ldots & & -a_0 \\ 1 & 0 & & & \vdots \\ & 1 & & & \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ & & & 0 & -a_{d-2} \\ & & & 1 & -a_{d-1} \end{vmatrix}$$

Then $\alpha + \alpha^2$ is represented by a matrix M with the form :

$$\begin{vmatrix} 0 & 0 & \ldots & & b_0 & c_0 \\ 1 & 0 & & & \vdots & \vdots \\ 1 & 1 & & & & \\ 0 & 1 & & & & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 1 & 1 & 0 & b_{d-3} & c_{d-3} \\ 0 & & 0 & 1 & 1 & b_{d-2} & c_{d-2} \\ 0 & & & 0 & 1 & b_{d-1} & c_{d-1} \end{vmatrix}$$

If the characteristic polynomial of M, i.e. Det $(M-\lambda I)$ has distinct roots, which is easily checked, then it is irreducible and its roots are $\alpha + \alpha^2$ and its conjugates. Here computing Det $(M - \lambda I)$ is an easy matter and essentially reduces to computing the determinant of a 2×2 matrix whose entries are polynomials in λ.

For, define by induction the matrix $P(\lambda)$ as follows :

$$P_{1,}(\lambda) = 1,\ P_{1,j}(\lambda) = 0,\ j = 2,\ldots,d\ ,\ P_{i,i}(\lambda) = \lambda P_{i-1,i-1}(\lambda),$$
$$i=2,\ldots,d\ ;$$
$$P_{i,j}(\lambda) = P_{i-1,j}(\lambda) + P_{i-1,j+1}(\lambda)$$

Then for $j > 1$, $i \geq j$ it is easily verified that :

$$P_{i,j}(\lambda) = \lambda\ P_{i-1,j-1}(\lambda).$$

Then, for $i \geq j$, we have that :

$$-\lambda P_{i-1,j-1}(\lambda) + P_{i-1,j}(\lambda) + P_{i-1,j+1}(\lambda) = 0$$

This shows that the matrix $P(\lambda)$ $(\lambda I-M)$ has the form :

$$\begin{vmatrix} \lambda & 0 & 0 & 0 & \ldots & 0 \\ 0 & \lambda^2 & 0 & 0 & \ldots & 0 \\ 0 & 0 & \lambda^3 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ & & & \lambda^{d-2} & 0 & 0 \\ 0 & \ldots & & Q_1(\lambda) & Q_2(\lambda) & \\ 0 & \ldots & & Q_3(\lambda) & Q_4(\lambda) & \end{vmatrix}$$

and consequently :

$$Q_1(\lambda)\ Q_4(\lambda) - Q_2(\lambda)\ Q_3(\lambda) = \lambda^{d-1}\ \ \mathrm{Det}(\lambda I-M).$$

An analoguous construction may be done for $\alpha + \alpha^3$ which reduces to computing the determinant of a 3×3 matrix.

Notice that the described transformation is performed in $O(d^2)$ operations in $\mathbb{F}_q$ after $P(\lambda)$ has been computed once for all. (Only the last two rows of $P(\lambda)$ are needed).

2.3. - Looking for primitive polynomials

Let α_1 be a root of $g_1(X)$, irreducible polynomial of degree d. Then if $g_i(X)$ is obtained from $g_{i-1}(X)$ by constructing the polynomial of which the roots are the conjugates of $\alpha_{i-1} - 1$, or $\alpha_{i-1} + \alpha_{i-1}^2$, or $\alpha_{i-1} + \alpha_{i-1}^3$ one of those transformations being taken at random and verifying each time that the obtained polynomial has distinct roots, we get a sequence of irreducible polynomials, each $g_i(X)$ being characterized by β^{j_i} which is the transformed of $\beta^{j_{i-1}}$ where β is a primitive root of $\mathbb{F}_q d$.

If we assume -but this is questionable- that j_i, i=1,2,... is a random sequence of integers in $[1,q^d-1]$, then the probability that $(j_i,q^d-1)=1$ is the probability that any two integers are relatively prime, which is $6/\Pi^2$ [9].

If moreover we know the small factors of q^d-1 up to s, then we are able to eliminate the polynomials $g_i(X)$ for which $1 < (j_i,q^d-1) < s$. If our assumption is reasonable, then by the argument of the theorem of CESARO already quoted [9] the probability for the rest of the polynomials to be primitive would be :

$$1/(1 + 1/(s+1)^2 + 1/(s+2)^2 + \ldots).$$

The fact could be checked statistically over irreducible polynomials of degree d for which the factors of q^d-1 are known.

APPENDIX

PROOF OF THEOREM 1

Denote $\mathbb{F}_q$ by K. By the chineese remainder theorem, the algebra $A = \mathbb{F}_q[X]/(f(X))$ is isomorphic to the product of k fields, each of which being isomorphic to $L \simeq K[X]/(f_i(X))$, where $f_i(X)$ is an irreducible factor of f(X) of degree t, i = 1,...,k.

Let $f_i(X) = \prod (X - \alpha_i^{q^j})$. It can be shown (for example [4]) that the mapping $w(X) \rightsquigarrow (w(\alpha_1), w(\alpha_2), \ldots w(\alpha_k)) = (\hat{w}_1, \hat{w}_2, \ldots \hat{w}_k)$ displays an isomorphism of A onto $\hat{A} = L \times L \times \ldots \times L$ of which the existence is announeed by the recalled theorem. In particular an idempotent u has components $\hat{u}_i$ in {0,1}, i = 1,...,k.

Now since the trace operator $T_{L/K}$ is surjective from L onto K, then for every i = 1,...,k, there exist an element in $\hat{A}$ of the form $(0,\ldots,0,\hat{w}_i,0,\ldots,0)$ for which $T_{L/K}(\hat{w}_i) = 1$. This means that there is a polynomial in A, w(X), such that $Tw(X) = w(X) + w(X^q) + \ldots + w(X^{q^{t-1}}) \in A$ is the primitive idempotent e_i. Now Tw has degree less than n. This proves in passing that $T\{1,X,X^2,\ldots X^{n-1}\} \subset$ A generates B over $\mathbb{F}_q$, since for $w(X) = \sum_{i<n} x_i X^i$, then $Tw = \sum_{i<n} x_i TX^i$.

On the other hand, let j in [1,...,k] be distinct from i. Then the algebra $A^* = K[X]/(f_i(X)f_j(X))$ is mapped isomorphically onto L × L by $a^*(X) \rightsquigarrow (a^*(\alpha_i), a^*(\alpha_j))$ as seen above. Thus for any polynomial g(X) and its remainder $g^*(X)$ mod $(f_i(X)f_j(X))$, then we have $(g(\alpha_i), g(\alpha_j)) = (g^*(\alpha_i), g^*(\alpha_j))$.

We can now write successively for s = i,j : $T_{L/K}\, w(\alpha_s) = T_{L/K}\, w^*(\alpha_s)$; $(Tw)(\alpha_s) = (Tw^*)(\alpha_s)$, with $Tw = \sum_{\ell<n} a_\ell TX^\ell$ and $Tw^* = \sum_{\ell<2t} b_\ell\, TX^\ell$. This shows that there exist an h < 2t such that $(TX^h)(\alpha_i) \neq (TX^h)(\alpha_j)$; in other words the element TX^h which is in B separates the dempotent $e_i + e_j$, which proves the theorem.

Theorem 3 : Let m be a product of two primes, m = ab, such that (q,m) = 1 and moreover such that q is primitive mod a and mod b. Let $F_m(X)$ be the cyclotomic polynomial with degree $\phi(m)$. Finally, let G, be the multiplicative subgroup generated by q in $\mathbb{Z}/m\mathbb{Z}$, with coset representatives

$s_1,\ldots,s_k$ in the group of units of $\mathbb{Z}/m\mathbb{Z}$. Then considering $F_m(X)$ as belonging to $\mathbb{F}_q[X]$, we have that $\{1, TX^{s_1}, \ldots, TX^{s_{k-1}}\}$ is a basis of the Berlekamp subalgebra B of $A = \mathbb{F}_q[X]/F_m(X)$.

Clearly $F_m(X)$ has k irreducible factors in $\mathbb{F}_q[X]$, each one of degree $t = \phi(m)/k = \text{Card } G_1$, since G_1 is isomorphic with the Galois group of every factor of $F_m(X)$.

Substituting the primitive m^{th} roots of one to X in X^s shows by the argument used in the preceeding proof that :

$$(X^{s \bmod m}) \bmod F_m(X) = X^s \bmod F_m(X)$$

(1) and

$$(TX^s) \bmod F_m(X) = (T(X^s \bmod F_m(X)) \bmod F_m(X).$$

Thus we have that : $TX^{s_i} = TX^{s_i q^j} \in A$, $i = 1,\ldots,k$; $j = 0,\ldots,t-1$;

where "$\in A$" tells that the considered polynomials are to be taken mod $F_m(X)$.

Now the set $T\{1,X,\ldots,X^{m-1}\}$ computed mod $(X^m - 1)$ spans by theorem 1 the Berlekamp subalgebra of $\mathbb{F}_q[X]/(X^m - 1)$ and consequently, reduced in A spans the Berlekamp subalgebra B of A. But, by hypothesis, $T_{L/K}\alpha^{sa} = T_{L/K}\alpha^{sb} = 1$, for every α primitive m^{th} root of unity and for every s with $(s,m)=1$. Consequently, $TX^{sb} = TX^{sa} = 1$, in A. On the other hand, $\sum_{1 \le j \le k} TX^{s_k}$ is, in A, also a constant in $\mathbb{F}_q$.

This shows that $\{T(1), TX, \ldots, TX^{m-1}\}$ spans the same subspace over $\mathbb{F}_q$ in A that $\{1, TX^{s_1}, \ldots, TX^{s_{k-1}}\}$. Since the rank of B over $\mathbb{F}_q$ is k, the theorem is proved.

Corollary. Let m be a product of two primes, $m = ab$; $(a-1,b-1) = 2$. If moreover 2 is primitive in $\mathbb{F}_a$ and in $\mathbb{F}_b$, then $(X + X^2 + \ldots + X^{2^{t-1}}, F_m(X))$ is an irreducible polynomial of degree $t = (a-1)(b-1)/2$ in $\mathbb{F}_2[X]$.

Since 2^{a-1} has order $(b-1)/2$ mod b, the order of 2 mod m is t as stated Now, by theorem 3, $\{1,TX\}$ is a basis of B which is spanned by the two primitive idempotents e_1, e_2 of A. Since then TX is not $e_1 + e_2 = 1$ and it should be e_i, $i = 1$ or 2. □

APPENDIX 2

CONSTRUCTING IRREDUCIBLE POLYNOMIALS

1. - BASIC PROPERTIES

Let K be a field and :

$$f(Z) = \sum_{o \le i \le d} \sigma_i Z^i \in K[Z],$$

with $\sigma_o = 1$ and $\sigma_d = 1$, $d > 0$. The given polynomial $f(Z)$ has distinct roots. Now consider the power series expansion :

$$(1) \qquad Z f'(Z)/f(Z) = - \sum_{i \in \mathbb{N}} a_i Z^i = P(Z)$$

with $a_o = 0$.

Let us then recall the following usefull facts.

Theorem. Consider the following properties L_1 and L_2 :

L_1 : The system of equalities

$$\begin{aligned} & a_1 + x_1 = 0 \\ & a_2 + x_1 a_1 + 2 x_2 = 0 \\ & \cdots\cdots\cdots\cdots\cdots \\ & a_d + x_1 a_{d-1} + \ldots + x_{d-1} a_1 + d\, x_d = 0. \end{aligned} \qquad (2)$$

has, for the sequence $a_1, \ldots, a_d$ given by the R.H.S. of (1), the unique solution $(x_1^\dagger, \ldots, x_d^\dagger)$.

L_2 : The system of equalities

$$\begin{aligned} & a_{d+1} + x_1 a_d + \ldots + x_d a_1 = 0 \\ & \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ & a_{2d} + x_1 a_{2d-1} + \ldots + x_d a_d = 0 \end{aligned} \qquad (3)$$

has the unique solution $(x_1,\ldots,x_d) = (\sigma_1,\ldots,\sigma_d)$.

We have that L_2 always holds and if L_1 is verified, then $(x_1^\dagger,\ldots,x_d^\dagger) = (\sigma_1,\ldots,\sigma_d)$

Proof : Let us first observe that L_1 is not always true. Indeed for $f(Z) = 1 + Z + Z^2 \in \mathbb{F}_2[Z]$, we see that x_2 is not determined. Since $(x_1,\ldots,x_d) = (\sigma_1,\ldots,\sigma_d)$ is a solution for (2), by (1), we are then left with proving L_2.

Consider the matrix :

$$C = \begin{vmatrix} 0 & 0 & \ldots & -\sigma_d \\ 1 & 0 & \ldots & -\sigma_{d-1} \\ & 1 & \ldots & \vdots \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots 1 & -\sigma_1 \end{vmatrix} \tag{4}$$

Since (3) is verified for $(x_1,\ldots,x_d) = (\sigma_1,\ldots,\sigma_d)$ as well as

$$a_{j+d} + \sigma_1 a_{j+d-1} + \ldots + \sigma_d a_j = 0, \forall j > d, \tag{5}$$

we then have :

$$(a_i, a_{i+1},\ldots,a_{i+d})\, C = (a_{i+1},a_{i+2},\ldots,a_{i+d+1}) \quad , \forall i \geq 1$$

Then if $(x_1^*,\ldots x_d^*)$ is a solution for (3), we have that

$$-(a_{d+1},\ldots,a_{2d}) = (a_1,\ldots,a_d)(x_d^* I + x_{d-1}^* C + \ldots + x_1^* C^{d-1})$$

and consequently :

$$-(a_{d+1},\ldots,a_{2d})\, C^i = (a_1,\ldots,a_d)\, C^i (x_d^* I + x_{d-1}^* C + \ldots + x_1^* C^{d-1}),$$

which shows that (5) holds when replacing $(\sigma_1,\ldots,\sigma_d)$ by $(x_1^*,\ldots,x_d^*)$.

This proves that $g(Z)\, P(Z)$ is a polynomial for $g(Z) = \sum_{o\leq i\leq d} x_i^* Z^i$ and $x_o^* = 1$. But $g(X)\, P(X) = g(X)\, f'(X)/f(X)$.

Now $f'(Z)$ is not zero and has no common factor with $f(Z)$. This implies that $g(Z) = f(Z)$. □

2. - RELATED PROPERTIES

The theorem just stated was presented in a form which is ready for use. However some other interesting properties may be derived straightforward from the argument of proof.

Let $h(Z)$ and $g(Z)$ be in $K[Z]$ with respective degree t and d, $t < d$ where $h(Z) \neq 0$ and $g(o) \neq 0$. We consider the power series expansion :

$$h(Z)/g(Z) = \sum_{i \in \mathbb{N}} b_i Z^i \tag{6}$$

Theorem. The so called Hankel matrix

$$H_n^{(d)} = \begin{vmatrix} b_n & b_{n+1} & \cdots & b_{n+d-1} \\ b_{n+1} & b_{n+2} & \cdots & b_{n+d} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n+d-1} & b_{n+d} & \cdots & b_{n+2d-2} \end{vmatrix} \tag{7}$$

is invertible over K for all n in $\mathbb{N}$ iff $(h(Z), g(Z)) = 1$. Moreover, for $K = \mathbb{Q}$, if there exist polynomials $s(Z)$ and $t(Z)$ in $\mathbb{Z}[Z]$ such that :

$$s(Z)\, h(Z) + t(Z)\, g(Z) = 1, \tag{8}$$

then $H_n^{(d)}$ is unimodular.

The first assertion follows from the preceeding proof. Now if (8) is verified, then $(h(Z), g(Z)) = 1$ in $\mathbb{F}_p[Z]$ for any finite field $\mathbb{F}_p$. Hence $\operatorname{Det} H_n^{(d)} \not\equiv 0 \bmod p$ for every prime p, which means that $H_n^{(d)}$ is unimodular. □

In P. CAMION [18], we proved (this follows from theorem 2 of that paper) that if n and n_2 are positive integers such that there exist primes p_1, p_2 with $p_1 \nmid n_1$, $p_1 | n_2$, $p_2 \nmid n_2$, $p_2 | n_1$, then there exist polynomials $E_1(Z)$, $E_2(Z) \in \mathbb{Z}[Z]$ with the property :

$$E_1(Z) F_{n_1}(Z) + E_2(Z) F_{n_2}(Z) = 1, \tag{9}$$

where $F_m(Z)$ denotes the cyclotomic polynomial with degree $\phi(m)$. Notice that the statement is best possible for cyclotomic polynomials. For, if $n_1 = pq$, $n_2 = p$, p and q primes, we have that :

(10) $$F_{pq}(Z)\ F_p(Z) = F_p(Z^q) \equiv (F_p(Z))^q \bmod q.$$

Consequently $F_{pq}(Z) \equiv (F_p(Z))^{q-1} \bmod q$, which forbid relation (9). We then have :

Corollary 1. If p_1p_2/n_1n_2 and $(n_1,n_2) \not\equiv 0(p_1),(p_2)$ and $\phi(n_1) < \phi(n_2)$, let $h(Z) = F_{n_1}(Z)$ and $g(Z) = F_{n_2}(Z)$ in (6). Then the matrix $H_n^{(\phi(n_2))}$ of (7) is unimodular for all n in $\mathbb{N}$.

Corollary 2. If $h(Z) = 1$ and if the polynomial $f(Z) \in \mathbb{Z}[Z]$ is monic with $|f(0)| = 1$, then the Hankel matrix of (7) is unimodular for all $n \in \mathbb{N}$.

Indeed, the denominator of $1/f(Z)$ has a non-zero constant term and has degree d in every ring $\mathbb{F}_p[X]$.

Example 1 : Let $h(Z) = 1$ and $g(Z) = 1 - Z - Z^2$, then the sequence $(b_i)_{i\in\mathbb{N}}$ in (6) is the Fibonacci sequence 1, 1, 2, 3, 5, ... and we have that :

$$|b_n^2 - b_{n-1}\ b_{n+1}| = 1.$$

Example 2 : Let $h(Z) = 1$ and $g(Z) = (1-Z)^d$. Then :

$$b_i = \binom{d-1+i}{d-1}$$

We then have that :

(12) $$\text{Det} \begin{vmatrix} \binom{n+k}{k} & \binom{n+k+1}{k} & \dots & \binom{n+2k}{k} \\ \binom{n+k+1}{k} & \binom{n+k+2}{k} & \dots & \binom{n+2k+1}{k} \\ \dots & \dots & \dots & \dots \\ \binom{n+2k}{k} & \binom{n+2k+1}{k} & \dots & \binom{n+3k}{k} \end{vmatrix} = \pm 1$$

for $n \geq 0$ and $k \geq 0$.

And then also :

$$(13)\qquad \operatorname{Det}\begin{vmatrix} \binom{n+k}{k} & \binom{n+k+1}{k} & \dots & \binom{n+2k}{k} \\ \binom{n+k}{k-1} & \binom{n+k+1}{k-1} & \dots & \binom{n+2k}{k-1} \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \binom{n+k}{0} & \binom{n+k+1}{0} & \dots & \binom{n+2k}{0} \end{vmatrix} = \pm 1$$

for $n \geq 0$, $k \geq 0$.

(13) is obtained from (12) by row transformations. Consequently (12) may be directly verified by modifying the matrix in (13) by column transformations.

Corollary 3. We have the general relation :

$$(14)\qquad \operatorname{Det} H_{n+j}^{(d)} = (-1)^{d+1} (-\sigma_d)^j \operatorname{Det} H_n^{(d)}$$

Moreover if $h(Z) = 1$ and if $g(Z)$ is a polynomial from $\mathbb{Z}[X]$ with $\sigma_0 = 1$ and $\sigma_d \neq 0$, then $\operatorname{Det} H_n^{(d)} \equiv 0 \bmod p$, for every prime divisor p of σ_d and $n \geq d$.

The relation $H_{n+j}^{(d)} = H_n^{(d)} C^j$ entails (14).

The second assertion follows from the fact that $1/g(Z) \bmod p$ has a denominator with degree less than d when $p \mid \sigma_d$.

BIBLIOGRAPHIE

[1] E.R. BERLEKAMP
"Factoring polynomials over finite fields",
Bell System Tech. J. 46 (1967) 1853-1859.

[2] E.R. BERLEKAMP
"Factoring polynomials over large finite fields"
Math. Comp. 24 (1970) 713-735.

[3] E.R. BERLEKAMP
"Algebraic Coding Theory"
Mac Graw-Hill (1968)

[4] P. CAMION
"Un algorithme de construction des idempotents primitifs d'idéaux d'algèbres sur $\mathbb{F}_q$"
C.R. Acad. Sc. Paris t. 291 (20 octobre 1980).

[5] P. CAMION
"Un algorithme de construction des idempotents primitifs d'idéaux d'algèbres sur $\mathbb{F}_q$"
Theory and Practice of Combinatorics, Annals of Discrete Mathematics
Submitted july 1980, to appear march 1982.

[6] P. CAMION
"A Deterministic Algorithm for Factorizing Polynomials of $\mathbb{F}_q[X]$"
To appear in proceedings of the International Colloquium on Graph Theory and Combinatories, Marseille Luminy June 1981. Annals of Discrete Mathematics (17), North-Holland Mathematics Studies, Vol.75.

[7] P. CAMION
"Codes quadratiques abéliens et plans inversifs miquéliens"
C.R. Acad. Sc. Paris, t. 284 (6 juin 1977).

[8] P. CAMION
"Factorisation des polynômes de $\mathbb{F}_q[X]$"
Revue du CETHEDEC, N.S. 812, 4ème trimestre 1981.

[9] D.E. KNUTH
The Art of Computer Programming, vol. 2
Seminumerical Algorithms. Reading Mass. ; Addison-Wesley (1971).

[10] R.J. Mac ELIECE
"Factorization of polynomials over finite fields"
Math. Comp. 23, 861-867.

[11] F.J. Mac WILLIAMS
"The structure and properties of binary cyclic alphabets"
Bell System Tech. J. 44 (1965), 303-332.

[12] M.O. RABIN
"Probabilitic Algorithms in finite fields"
MIT/LCS/TR-213 (Jan. 1979).

[13] K.P. ZIMMERMAN and K.K. TZENG,
"Lagrange's interpolation formula and generalized Goppa Codes".
Preprint.

[14] R.T. MOENCK
"On the Efficiency of Algorithms for Polynomial Factoring"
Math. Comp. 31, 235-250 (1977).

[15] D. LAZARD
"Factorisation des polynômes"
Rapport Université de Poitiers, 86022 Poitiers Cédex.

[16] P. FLAJOLET et J.M. STEYART
"A Branching Process Arising on Dynamic Hashing, Trie Searching and Polynomial Factorization".
Submitted to the 9th ICALP Symposium, Aarhus (1982)

[17] F.J. Mac WILLIAMS and N.J. SLOANE
"The theory of error correcting codes"
North Holland (1977).

[18] P. CAMION
"Unimodular modules and cyclotomic polynomials in Error correcting codes"
Edited by Henry B. MANN, John Wiley & Sons, Dec. 1969.

[19] A.V. AHO, J.E. HOPCROFT et J.O. ULLMAN
"The Design and Analysis of Algorithms"
Addison-Wesley Pub., Reading, Mars 1974.

Imprimé en France
par
l'Institut National de Recherche en Informatique et en Automatique